Identity based Blind Signature Scheme based upon DLP

Lokendra Rewapati

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India

Identity based Blind Signature Scheme based upon DLP

Dissertation submitted in the partial fulllment of the requirements

for the degree of Master of Technology

to the department of

Computer Science and Engineering

of

National Institute of Technology Rourkela

by

Lokendra Rewapati

(Roll 212CS2114)

under the supervision of

Dr. Sujata Mohanty

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India

dedicated to my Grandmother, Parents and Sister...

Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, India. www.nitrkl.ac.in

Dr. Sujata Mohanty
Asst. Professor

May , 2014

Certificate

This is to certify that the work in the thesis entitled *Identity Based Blind Signature Using DLP* by *Lokendra Rewapati*, bearing roll number 212CS2114, is a record of an original research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of *Master of Technology* in *Computer Science and Engineering*. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Dr. Sujata Mohanty

Acknowledgement

This dissertation, though an individual work, has benefited in various ways from several people. Whilst it would be simple to name them all, it would not be easy to thank them enough.

The enthusiastic guidance and support of *Asst. Prof. Sujata Mohanty* inspired me to stretch beyond my limits. Her profound insight has guided my thinking to improve the final product. My solemnest gratefulness to her.

I am also grateful to *Prof. Banshidhar Majhi* for his ceaseless support throughout my research work. My sincere thanks to *Prof. Rameswar Baliarsigh* for his continuous encouragement and invaluable advice.

It is indeed a privilege to be associated with people like *Prof. S. K. Rath*, *Prof. S.K.Jena*, *Prof. D. P. Mohapatra*, *Prof. A. K. Turuk*, *Prof. S.Chinara*, *Prof. Pankaj Sa* and *Prof. B. D. Sahoo*. They have made available their support in a number of ways.

Many thanks to my comrades and fellow research colleagues. It gives me a sense of happiness to be with you all. Special thanks to *Dinesh, Aknan, Mahesh,Priyanka and Naveen* whose support gave a new breath to my research.
My Special thanks to Seema Bharti who always support me in times when i goes down,she motivate me in every situation.
Finally, my heartfelt thanks for her unconditional love and support. Words fail me to express my gratitude to my beloved parents who sacrificed their comfort for my betterment.

Lokendra Rewapati

Author's Declaration

I hereby declare that all work contained in this report is my own work unless otherwise acknowledged. Also, all of my work has not been submitted for any academic degree. All sources of quoted information has been acknowledged by means of appropriate reference.

Lokendra Rewapati
Roll: 212CS2114
Department of Computer Science
National Institute of Technology,Rourkela

Abstract

Blind Signature scheme deals with the concept where requester sends the request that the signer should sign on a blind message.Anyone can verify the signature after publishing the information without any restriction.The proposed scheme having the property of both concept, Identity based as well as Blind Signature using DLP.

With the help of Identity Based system we can easily archive the public key certification without key-management setting. In several ID based scheme ID map into an Elliptic curve, but we have a novel techniques to solve this problem. We have proposed a scheme that is based on Discrete logarithm problem.We have proved that our scheme meets all essential and secondary security prematurity.In addition we have given the mathematically and pragmatically correctness of our scheme. As our best of knowledge, we give the first discussion on these two notation. Also, we proved that our scheme fulfill all criteria that should be meet in a blind signature scheme.Our proposed scheme can be used in an E-commerce, E-voting and E-cashing anywhere without any restriction.We have given an application of E-cashing using our scheme.

***Keywords*:** Blind Signature, E-voting, Key- Management,DLP,Correctness.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

A digital signature is basically a way which provides the authenticity to an electronic document. A data stream concatenates a message with a valid entity called digital signature. The concept of Digital Signature is first have given in new direction cryptography by Diffie and hellaman [30]. Authenticity ensure the legitimacy of document as well as the person who created it. It also gives a guarantee that not any other person changed it since an authentic people developed it.

Digital signatures count on some kind of encryption to give a guarantee of authenticity. Encryption is a method in which we convert to message or file in such a format that when we send to it from one system to be other then no one decrypt it except the person who possess a key. Authentication ensured that the message that we get come from a right person. Digital signature shows that the data which we receive coming from a right people, it also showed a message cannot be denied or alter by a sender later the submission. Digital signatures are basically applied for financial transaction, distribution of software, in cases of controversy where we want to check for tempering of digital information [13].

Blind Signature is a technique in which a user can get the sign on document from a signer without showing the information that it stored [14]. In Blind Signature technique, the basic motive is getting the signature from a person without revealing secret information that document possessed. The property of

Blind Signature is that requester can be enabled to get the signature, but the signer party does not have any capability of making relation between signature and document. When requester released the signature pair, both requester and signer will not be able to link their pair. Apart from authentication blind signature also satisfied Unforgeability, untraceability also [1, 2, 7, 8, 11–14, 22]. The blind signature scheme should preserve the following requirement:

- **Blindness** The message should be blind for a signer, on the other hand, we can say that signer also not disguised the original content.
- **Unforgeable** An adversary even if he can imitate the user and freely interact to the signer must not produce or copy a true signs on other documents except for that signer signed.
- **Correctness** The Blind signature scheme must be correct.
- **Unlinkablity** A malicious signer must not be able to link output final signature to the user for separate interaction with the user.

1.1 Framework of ID-Based Blind Signature

The concept of Identity-based scheme removed the need for a requester or sender to look up the recipients public key before sending out an encrypted message [1, 4, 11]. Identity-based cryptography provides a good convenient alternative to conventional public-key infrastructures. An IDBS scheme consists of following four phases [24].

Setup : The Key Generation Center runs to this phase on input, and makes the public parameter's prams of the scheme and a master challenge. Key Generation Center publishes prams and retains the master unrevealed to itself.

Extract: For Given master secret, prams and identity ID, this phase created the secret key S_{ID}.

Issue: The signer put a signature blindly for a person by the present scheme, which

is further broken into three phases ($Blind, BlindSign, Unblind$).

Blind : User chooses some random string α or β for a given message m, it generates an output with the help of hash function, let's called it m' and transfer it to the person who had been signing authority. Sometimes, signer's interactive help needed by user.

Blind Sign: In Blind Sign phase, as an input insert the signers private key s_{ID} that he used for signing the message and blind message m' then in output it makes a blind signature σ' and transfers it to user.

Unblind : It generates the unblinded signature σ, for Given signature $\acute{\sigma}$ and random string α or β that used previously.

Verify : Given an identity ID, a message m, a signature σ and prams, this phase output true if σ is a valid signature on m for identity ID, elsewhere false.

1.2 Basic Security Feature of ID-Based Blind Signature Scheme

An IDBS should consist the following features Unforgeability, blindness and correctness. These features are listed as bellow [20, 21]:

Definition 1 *Correctness:*Suppose a requester and a signer agree with an ID-based blind signature protocol, then probability $1 - (1 \div (t^c))$, where t is a security parameter, and c is a constant [29].Signer output and requesters outcome a s must fulfill $\text{sv}(s, ID, m, publicparameters) = accept$. The probability calculated over the randomness of setup, key generation and signature generation.

Definition 2 *Blindness:*IDBS scheme said to satisfied blindness feature when all selective polynomial time attacker $A^{'}$, $A^{'}$ says wins if and only if the wins getting with at most the probability $(\frac{1}{2} + \frac{1}{t^c})$,where t is a large number and c is a constant. The calculation of above equation over the randomness of attacker and v_0 and v_1 [29]. The blindness is a property of an IDBS scheme may be given through this way.An attacker or malicious user let's say $A^{'}$,(v_0, v_1) are two requesters.

1. After getting public parameters param adversary can choose a random identity

ID and (m_0, m_1) two messages.

2. Adversary $A^{'}$,selects $n \in 0, 1$ randomly and kept n as private. After that, $A^{'}$ sends $(m_n, ID, param)$ to the requester v_0 and $(m_{1.n}, ID, param)$ to the requester v_1 respectively.

3. Now $A^{'}$ execute the blind signature phase for (v_0, v_1).

4. If output of v_0 and v_1 along with true signature (m_n, ID, σ_0) and $(m_{1.n}, ID, \sigma_1)$ than it will be sent (σ_0, σ_1) to $A^{'}$ else give nothing to $A^{'}$.

5. Adversary $A^{'}$ computes output and if gets $n^{'} \in 0, 1$ than we will say adversary wins if $(n^{'}, n)$.

Definition 3 *Ungorgeability:* An attacker is known as a forger if he/she having a tuple(P, t, Q_e, Q_s) for an IDBS scheme where in at most time t with at least probability P using the number of times key generation Q_e should have gotten at most Q_s times blind signature issuing phase. This is a sufficient and necessary condition for declaring an attacker as a forger. On the other hand, we can declare a blind signature scheme as an unforgeable if and only if there should not present a two tuple (P, t, Q_e, Q_s) with same property.

The unforgeability property of IDBS scheme is given by the following game between a malicious requester and challenger [20, 21, 29].

Setup: The challenger carries out the algorithm set of the identity-based blind signature process and acquires both the master secret and public parameters. The malicious requester is given public parameters, and master secret is kept by champion.

Queries: The malicious requester can use two kinds of queries in a randomly concurrent and loop way.

Key Generation Queries: The spiteful requester or attacker can be asked for the master key of any identity(ID) of their choice. The challenger executed the key generation phase and calculates a master key for every query of ID to the spiteful requester.

Blind Signature Issue Related Queries: The spiteful requester may be requested for blind signature of any ID on any message of his /her choice in an interleaving and concurrent way. Challenger executed the key generating phase

$kg(params, ID)$ for each and every query of blind signature to get the secret key d_{ID} of ID.After that the Challenger executed the blind signature issuing phase with malicious requester. Where the malicious requester plays a role of requester, and challenger plays the role of original signer.

Suppose $n^{'}$ is a number of runs of the blind signature signing phase where output completed by challenger [18].time k is in the polynomial time where both get to stop the process.

Forgery: We will declare a malicious user as a winner of game if he gets the ultimately list of output as a valid signature l is $(\sigma_1, ID_1, m_1).....(\sigma_i, ID_i, m_i)$ such that:

1. It should be $l > l^{'}$.
2. For every topple of $i = 1, 2, ...l$, $sv(m_i, \sigma_i, param_i, ID_i) = accept$.
3. The malicious user had not designed a key generating query for any $ID_i, i \in \langle 1...l \rangle$.
4. $(m_i, ID_i) = (m_j, ID_j)$ for each topple of (i, j) with $i \neq j$ where $\forall i, j \in \langle 1...l \rangle$.

At the last, we will say $M_{inforge}$ to be a probability of an attacker wins the game. Here the condition of probability is picking up over the toss of every coin design by Malicious user and challenger.

1.3 Application of ID-Based Blind Signature

1.3.1 E-Voting System

E-voting is a most important application of blind signature scheme [21,48].To cast vote and counting the electronic vote is known as electronic voting. In fig, voter is free from of any fair because he/she put cast their vote blindly admin is nothing but the authority who provides the sign. E-voting application may be organized by any government representative, private organization, or any special group of people. The privacy of user who cast the vote is keeping blind. Every user's cast vote can be easily verified with the help of admin's identity. The confidentiality issue related to digital signature is a bit solved by IDBS scheme.

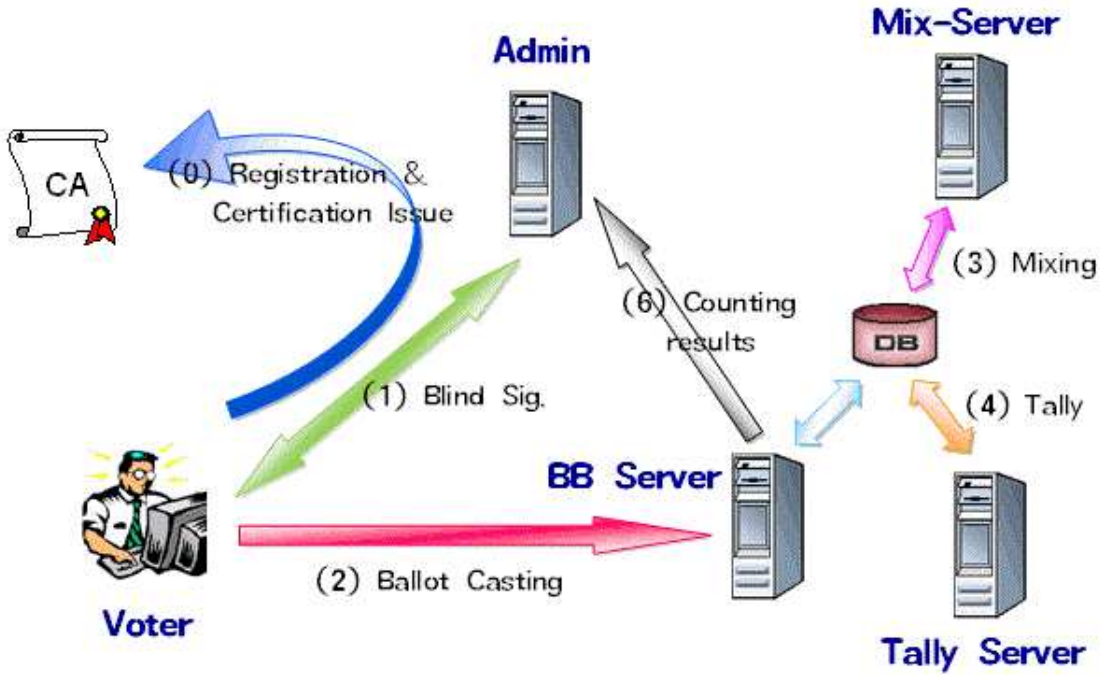

Figure 1.1: E-voting System using BS

1.3.2 E-cashing System

E-cashing is most concern applications of IDBS scheme, in given fig we show the process how does use it [20].E-cashing consisting selling and buying of products or services over the Internet and open network [9].IDBS scheme is a simply has been used in today's competitive market. In fig, we have shown all the process that will be a good application of our scheme. An android based application have been designed using IDBS idea in fig.User have to execute blind signature and verify phase and the merchant distinguished with a bank's authority. We will design our concept in the future for this application.

1.3.3 E-Business

E-Business is a combination of "e-mail" and "e-commerce".Both services conduct under the open network or in the Internet, the selling and a significant part of the early worry about the security of a business transaction on the Web, can be solved with IDBS system.

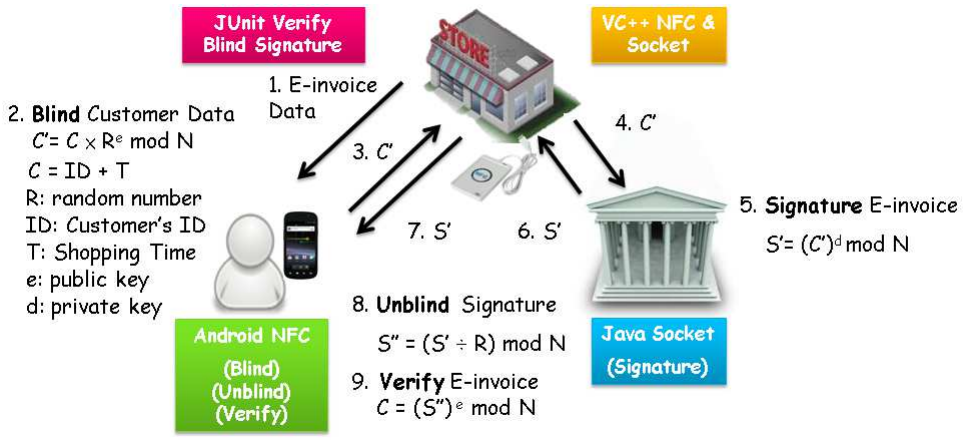

Figure 1.2: E-cashing using BS

1.4 Motivation and Objective

We have been understanding the importance and digital signature in every aspect of information technology. In 90s the idea of DS is extended into BS [12].There is a large number of IDBS schemes based on ECDLP, Bilinear have been proposed but the problem is, that either we have to compromise with high computation complexity or some security fault [1, 4, 7–9, 11, 20, 21, 24, 29].So our clear objective to make a scheme with the better security features along with low computation overhead. So we have to define an algorithm based on DLP using ID based idea.

1.5 Problem Statement

The main goal of our design is given as listed below:

a IDBS scheme consisting DLP assumption.

b IDBS scheme should not be affected by a malicious user or cheater signer.

c It should meet all the security feature properly.

d The computation overhead should be low.

e The third party authentication also be encountered.

f IDBS scheme must fulfill all the requirements namely correctness,Unforgeability,unlink ability,and blindness.

1.6 Organization of Thesis

This thesis has been consisting in six parts. Chapter 1 is followed by survey of IDBS scheme along with BS survey, and DS survey and their classification. In chapter 3, we have given the proposed algorithm. The security analysis and computation complexity describe in chapter 4. Result and Implementation idea given in chapter 5. Finally, conclusion and future work of a proposed scheme are given in chapter 6.

Chapter 2

Literature Survey

In this section, we reviewed the literature related to different blind signature schemes and their security features. First, we give a brief overview of digital signature, then preliminaries related to blind signature, hash function, random number function,random number generation, prime number with primality test, and some basic concepts of cryptography. Survey on different blind signature scheme and IDBS scheme have been given in the middle, At the end,we reviewed some popular IDBS schemes, and their classification based on security features.

2.1 Cryptography Concepts, Digital Signature Signature and Blind Signature Requirement

Cryptography is a technique by which we can send our data protectively in open network [22].Cryptography implies "secret writing",a art and science of transferring information to make them secure and immune from attacks. On the sender side plain text or original text, firstly, encrypted on chipper-text and it will be decrypted on the receiver end in the form of plain text.
Cryptography basically divides into three measure part.

1. **Symmetric key encipherment:** In this technique, both senders as well as a receiver has the single key, and used it for cryptographic operation.

2. **Asymmetric key enchiperment:** These techniques also known as public-key enchiperment where a sender used the public key of a receiver, and receiver used his own private key for deciphering data.

3. **Hashing:** A variable length message converts or maps into fixed size message digest [13, 19]. The digest generally much smaller than the original message.

2.1.1 Cryptographic Hash Function

It is a well-defined algorithm which can be applied on a group of data or piece of information, often a single file, generating a value called checksum [19].It always producing the result of fixed length from an arbitrary length of block such that any minor change would be a very elevated change the value of hash with a elevated probability. The input piece of information to be encoded is called as message and the output of hash function is said to be as message digest [30]. Generally a valid hash function consists some most important properties they are described as first hash function should have a primage resistance that implies if a granted hash key h it is very difficult to get any message m like $h = hash(l, m)$, l is here the hash key [6, 13]. Second is hash function should have a good enough collision resistance it shows if two given message m_1, m_2 it is completely impossible to get hash h such that $h = hash(l_1, m_1) = hash(l_2, m_2)$, where l_1,l_2 are two hash keys. The third property is a hash function should have second primage resistance that means if a given message m_1, such that $hash(l, m_1) = hash(l, m_2)$,where l is a hash key.

2.1.2 Prime Numbers and Primarility Tests

Primes are a special number in the family of integers because they are numbers that do not have any non-trivial factors. Large prime numbers are used in most cryptographic algorithms, and they have grown increasingly important for this reason. Primality test is a method for determining whether a given input is prime

or not [31]. It always shows the statics of a prime number, whether it is, this did not give us any information about the factorization. The reason for using a prime number because it ensured us that our choose number have not any other factor. Factorization is a computational hard problem so finding whether the number is prime is comparatively easy. Primality test basically divides into two categories deterministic and probabilistic. Deterministic primality testing except integer as an input and output is a prime or composite number. Deterministic test determined based on absoluteness, whether a given number is prime. Till date of today, there is no algorithm that would be feasible use for a large prime number. In 2002, kayal and agrawal saxena proposed a scheme that performed primarily tests on polynomial time [32].

Probabilistic testing based on uncertainty of a prime number that means we said a number is probable prime till their primality may be demonstrated deterministic-ally. This testing is much faster than deterministic [31].

2.1.3 Survey on Digital Signature Schemes

Digital signature is a method to conform the agreement of message [30].It is the signature which only generated by signer and verifies by anyone in the network through the protocol. The digital signature provides three basic requirements of security but not the confidentiality, so it can be achieved with the help of blindness of original information but the way of working gave only confidentiality between user and signer.

Digital Signature must follow the two basic requirements [19, 26, 30, 33]:

Unforgeable: If a signer signed a document D with the signature σ, no one can produce the same message signature pair(σ, D).it ensured that there would not be any other message signature pair with same value rather than an original message.

Authentic: If a signer signed a message M, then receiver or any other would verify it, if he knows the public key of signer.The recipient convinced deliberately to signer.

A digital signature should not be alterable, reusable and non-repudiation [33]. In 1984, R.L.rivest, presented a method for obtaining digital signature [34]. This was a method where encryption key's open nature does not reveal the subsequent decryption key. This proposal opened the door for new system known as the public-key system.

In 1999, a modern proposal was given based on digital signature in RSA that was a combined design of fault tolerance and hash function and digital signature [33].Later on in 2003, Afzel Moore had proposed a new approach of conditional access system architecture [35].XML digital signature were used in order to distribute video, image data and audio file on the web in a encrypted manner.

In 2005, Gulin Wang proposed a new idea where the trusted third party is involved when the one-party cheating or communication channel is interrupted [33].In 2008, For an E-mechanism the use of secure crypto-environment being the important issue of information security. All these these requirements might be fulfilled with the integrated design based on SoC;Design was implemented with SHA-2 using public-key cryptosystem [36]. A reconfigure hardware having a core logic used with 2048 bits RSA digital signature scheme.

Later in 2008, Ming-Hsin Chang, adapted a new concept in a digital signature world through only using ECDSA. Even using ECDSA and DSA still there were lacked of characteristics of proxy signature, Ming has achieve a proxy delegation with the help of only ECDSA [37]. A fast ECC based digital signature using DSP scheme proposed by Ying Qin, where a variable window mechanism used, therefore, combining NAF and sliding window with varying length reduce to complexity of point multiplication of ECC [38].In 2010, a one-time authentication approach has been proposed, which allow an owner to grant his right to a temporary user without giving any actual information related to original password [33].

In 2011, an unfeasible problem had been solved those were the preserving transparency and optimistic fair exchange [39]. The role of secure trusted third party to being involved if required and transparent for affluent. This was the best technique for solving a real-world problem. E-governance is the successful

application being developed with this methodology.

2.1.4 Survey on Blind Signature

The idea of blind signature has been proposed in 1983, based on RSA algorithm [**?**].The main application of it to protect user's privacy in the open network e.g.an E-business, E-governance, E-case,E-voting systems [20, 22].In Digital Signature, there are only two participants knows as signer and verifier used, but in a blind signature scheme, three participants involved namely verifier,user,signer. First of all,user or requester blinds the message with the help of some random parameters and hash function. After getting the blind message signer will put the sign on the message by applying his/her private key. Once the message signed by the signer it sends back to the requester he/she unblind the message and submit it to the verifier. After receiving the message-signature pair verifier used public key of legitimate signer and verify it.
The basic differences in blind and digital signature are listed below [2]:

1. Message content needed not to be blind in digital signature from the signer, but in a blind signature, it should be blind.

2. After publishing signature on a message signer ought not have the capacity of linking the signature to message.

The basic characteristics that blind signature should possess are unforgeability,correctness,blindness and untraceability.

2.1.5 Basic Concept of Blind Signature

In 1983, D. Chaum gave the idea of blind signature. This technique ensured the secrecy of user [**?**]. In this approach two parties involved, one user A and other signer B. User A wants sign on a message M by signer B. User, firstly, used hash function on message M and changes to it in $M^{'}$, and transfer it to a signer. Signer creating the signature $s^{'}$ and put into $M^{'}$ and sends back to A. After

getting s' user A unblinds into s this is nothing but the signature on a message M.So user A protect the information and not to be revealed. On the other hand, signer assigned a message signature pair (M, s), signer neither able in finding the information about user for he sign a message nor about message.

Later on one-year D.chaum come with a new blind signature approach using RSA. This approach consists three parties along with five phases that were namely as Initializing,Blinding,Signing,Unblinding and Verifying.

The problem was with this scheme that the true blindness as well as unforgeability not achieved.

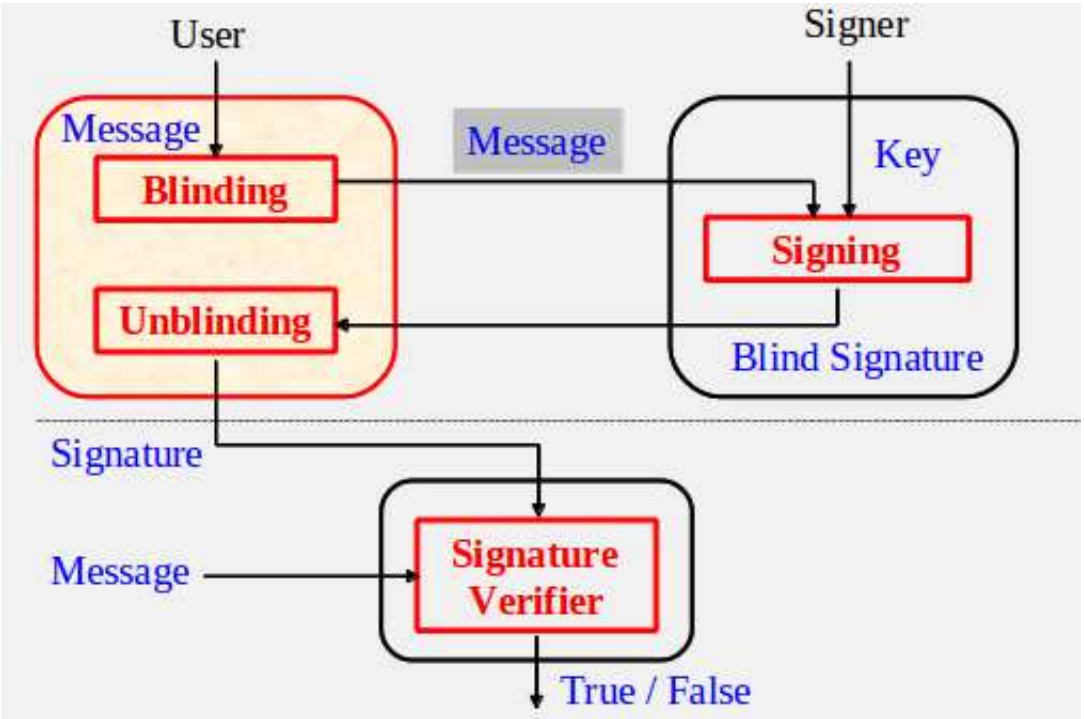

Figure 2.1: Blind Signature Process.

In 2001, Y.M.Tseng et al. came with a blind signature approach that depended on factoring problem [40].The problem with this approach was a large key size required otherwise an adversary can forge the signature. The same problem with this scheme also exit's signer can trace the message. In 2003, C.C. Lee, presented an untraceable blind signature scheme based on integer factorizing problem and Extended Euclidean algorithm. This scheme has been satisfied

untraceable property, but the problem where high overhead and long key size required for safeness [41].

In 1994, M. A. Stadler et al. al. proposed first Discrete logarithm based blind signature approach [2]. They presented two new blind signature scheme in their proposal. The first one was blind signature scheme generated from a little alteration of Digital Signature Algorithm. Second was based on The Nyberg-Repels signature scheme. L .harm in 1995 announced that the blind signature derived from DSA was providing not a true blind signature [42].Signer can keep the message signature pair and after publishing the message signature pair he/she can trace.Therefore,Camenic's scheme did not satisfy the untraceable property. Later on, on E. Mogammed and E. Emarah proposed a scheme had less computational complexity and better in time from a technique that based on the RSA algorithm [14].The problem with this scheme that in unblinding phase requester has to keep some parameter and on the base of this, he can easily get the private key of signer. So this scheme also did not satisfy the unforgeability. In 2010, a novel blind signature scheme presented by R.L.SHEN that derived from discrete logarithm problem [43]. This scheme was satisfied all basic requirements.

2.2 Survey on ID Based Blind Signature Schemes

IDBS approach being much more important since the public key of ones is simply used as his identity. For example, example A real-life example is, if an electronic case issued by the bank can be easily verified with the help of his identity it can be anything may be a combination of string like banks name, city, country, and year by any user or shops. They do not require to access or fetch a bank's key from PK center. Generic parallel attack is an open problem for schemes, based on IFP of RSA scheme.

In 1984, Shamir comes with Identity-based cryptography concept [**?**]. The

unique quality of this approach is that a users public key may be any binary string. It can be an email address or any unique constraint that can identify the user or signer.

The concept of Identity-based scheme removed the need for a requester or sender to look up the recipients public key before sending out an encrypted message. Identity-based cryptography provides a good convenient alternative to conventional public-key insfrastured [11, 19]. There are many identity-based signature schemes [1, 4, 7, 8, 11, 20, 21, 24, 29] have been proposed since 1984, but only appeared was in 2001 that was satisfied Identity-based encryption [45]. The advantage of ID Based scheme is that it simplified the process of key management. In the past couple of the year, there are several bilinear paring has been applied to various applications in cryptography [11, 17, 44].

The first IDBS scheme was proposed by Zhang and Kim, in 2002 [46]. The security of their scheme depends on the factorization of ROS problem. In 2002, Wagner claimed that the security of Zhang Kims scheme can be broken within time to break ROS problem. In 2002, K. Kim presented a scheme, but it was inefficient to implement and resistance against parallel attack was still not solved. Later in 2003 Zhang and Kim proposed a new ID based scheme that based on bilinear paring [47]. They claimed that their scheme is not depended on ROS problem. Huang et al. proposed an efficient IBBS scheme was more forgeable under problem is solvable. In 2010, Hu and Huang and Zhang et al. proposed an IBBS scheme in a standard model [29]. We prove that our scheme has existential unforgeability under the computation Diffe-Hellman assumption. Our scheme is very useful to develop an e-cash system.

2.2.1 Classification of ID-Based Blind Signature

There are five types are schemes that are mainly divided into five categories:

1. **ID Based Blind Signature:** These schemes are based on a simple blind signature concept, only change is that instead of public-key signer's ID used

for verification process.No need to manage a PKI unit at all. ID can be used by anyone for verification purpose [1, 4, 8, 9, 29].

2. **ID Based Restrictive Blind Signature:** Restrictive blind signature schemes which allow a user to receive a signed message without getting to reveal his private content of the message, but the selection of the message should be restricted. It should follows some constraint.

3. **ID Based Partially Blind Signature:**Signer should explicitly add some extra information. Extra information can be anything, date of expiration, time stamp, or whatever.On the resultant signature under some prerequisite agreement with user [23].

   In 2007, a partial blind signature concept was given efficiently than had less computation complexity and equal privacy concern than Chan et al's scheme [21]. Chan's scheme does not satisfy the restrictiveness and double spending problem.

4. **ID Based Restrictive partially Blind Signature:** Restrictiveness and partially both are an important security concerns on cryptography. A blind signature scheme which is based on this two property called IDPR-blind signature [20, 21, 23, 24].Fangguo Zhang claimed that their scheme was secure(provably) in the random oracle model [20].Their scheme was used to build an off-line, an untraceable E-cash system.

5. **ID Based Proxy Blind Signature:** A proxy signer used his/her private key for signature instead of original signer. This is a combination of proxy and blind signature concept. In 2008, first proxy based scheme was given but the problem with the scheme, it does not fulfill the untraceability property [15]. The proxy signer can forge the secret key of original signer and grant the authorities to others. In 2011, Ni Zhang had presented an efficient scheme that satisfied the untraceability [49].In 2013, a more feasible and secure ECDLP based scheme presented by sundram which solved a common problem of revoke of delegation by original signer [50].

2.3 Chapter Summary

The review of various ID- Based signature given us the real concept for enhanced security feature to be adaptable in the really world.ID-Based system has no need of PKD. Any entity's public key can be used as his/her identity. Signature can be verified with signer's identity instead of public key. The most reliable attack traceability, forgeability has found on various schemes. Many schemes provided a secured system but failed due to computation complexity and in-feasibility of implementation. Thus after reviewing the different kind of schemes proposed till the date, we have given a new concept that is low computational overhead and satisfied all security requirements.

Chapter 3

Identity Based Blind Signature Scheme based upon DLP

We proposed a Novel IDBS scheme, which provides untraceability,unforgeability and blindness to every entity. A secure trusted third party involved in proposed technique who initiates the blinding process. Identity of signer is used for verification of signature.

3.1 Proposed Scheme

The proposed IDBS Scheme consists of three participants namely, Trusted third party, Signer,User.The scheme having been following Six phases.

Table 3.1: Parameters used in the proposed scheme

Parameter	Function
p	A large prime number
q	A large prime factor of $(p-1)$
g	An element(generator) of Z_n^*
X_A	The secret key of the trusted party
Y_A	The public key of the trusted party where $Y_A = g^{X_A} mod p$
$H(.)$	A secure one way hash function

3.1.1 Setup Phase

The trusted party chooses p as a large prime and q as a prime factor of $(p-1)$,after that he chooses g as a generator in Z_n^*. The trusted party chooses his secret key X_A in Z_n^* and computes his public key Y_A as

$$Y_A = g^{X_A} mod p \tag{3.1}$$

The trusted party random select k in Z_n^* and computes

$$r = g^k mod p \tag{3.2}$$

$$S_s = (k + rX_A) mod p \tag{3.3}$$

trusted party then sends (r, S_s) to the signer so that he can calculate his ID and authenticity of a trusted party.

3.1.2 Extract

The signer checks trusted party's authentication as follows. $g^{S_s} = r.Y_A^r (g^k.g^{r*X_A} = r * Y_A^r)$ If the particular parameter given by trusted party is authenticated, then than he chooses X_B in random in Z_n^* and computes Y_B as a parameter

$$Y_B = g^{X_B} mod p \tag{3.4}$$

in a continuation signer computes the secret key for signing purpose $s = S_s + X_B mod p$ and the identity that will be used for verification purpose. The ID of signer calculated as

$$ID_B = g^s mod p \tag{3.5}$$

3.1.3 Blinding

The signer executes following protocol with user. The signer has been provided some agreement parameter so that user can blind his original message with some restriction. The signer chooses $l, t_R \in Z_n^*$ and computes $t_3 = g^{-s} mod p$

$$t_1 = X_B * (l)^{-1} mod p \tag{3.6}$$

$$t_2 = s * (X_B)^{-1} modp \tag{3.7}$$

$$\mu = g^l modp \tag{3.8}$$

and send (μ, t_1, t_2, t_3) to the user.

The user chooses α, β in random fashion in Z_n^* and computes

$$\dot{t} = H(m, \mu^{t_1} Y_B^{t_2} g^{-\alpha} \mu t_3^{\beta}) modp \tag{3.9}$$

$$t = \dot{t} + \beta * modq \tag{3.10}$$

and send t to the signer.

3.1.4 Signing

After receiving t signer use his secret key and sign the blind content that provides by the user. Signer computes

$$\dot{s} = (l - ts) modp \tag{3.11}$$

and send $\dot{s}$ the user.

3.1.5 Unblinding

After receiving $\dot{s}$, the signed blind content user applied his random selected parameter for unblinking the message, and he get the signature along with their original message without losing his secret.Than the user computes

$$\ddot{s} = (\dot{s} - \alpha) modq \tag{3.12}$$

$(\ddot{s}, \dot{t}, ID_B)$ This is nothing but the ID along with massage m.

3.1.6 Verification

After receiving $(\ddot{s}, \dot{t}, ID_B)$, anyone publicly can verify the signature by using the ID_B.

The verifier computes $\dot{t}$ as

$$\dot{t} = H(m, Y_B ID_B^{(1+\dot{t})} g^{\ddot{s}}) modp \tag{3.13}$$

Check if $(t' = t)$.,than the signature is valid and acceptable otherwise it should be rejected.

The message exchanging process or logical view of our scheme is given in below fig.

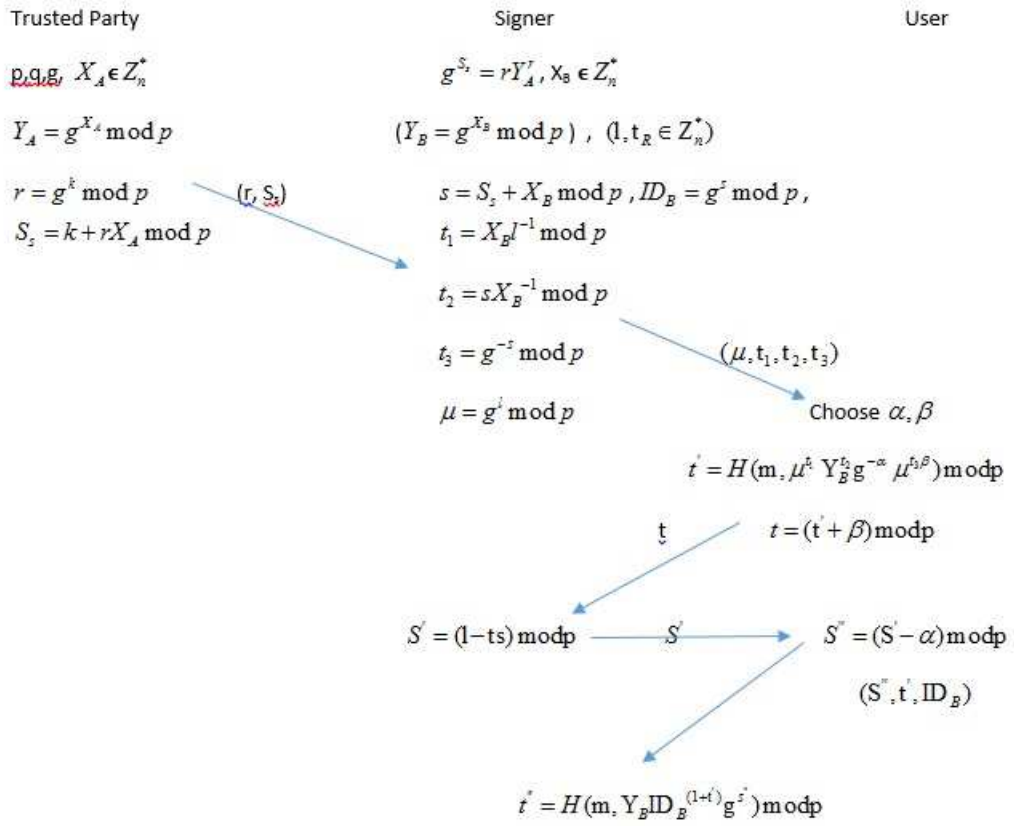

Figure 3.1: The step by step view of our algorithm

3.2 Chapter Summary

Our proposed scheme has been given in above work. Our scheme is based on DLP, which is declared as a computational hard problem. We combined unit of two features BS and ID. ID of signer is used for verification purpose that will remove the need of PKI and extra overhead.All the working steps shown in a sequence in the above sections.

Chapter 4

Security Analysis of Proposed Algorithm

4.1 Security Analysis of Proposed Scheme

The security of the proposed work based upon complexity of solve computational hard assumption such as DLP,IFP,CDHP.

4.1.1 Discrete Logarithm Problem

Discrete Logarithm Problem: Given $amodp$ or $a^n modp$ find n, put it in another way we need to compute $\log_a b$ where $a, b, p \epsilon Z_p^*$ this is called discrete logarithm problem. As we know DLP is an example of Computation hard problem it is impossible to solve [1, 2, 7, 10, 13].
The public key of the trusted party is calculated as

$$Y_A = g^{X_A} modp \tag{4.1}$$

this shows the discrete logarithm problem so for calculating X_A we need to calculate the discrete logarithm of Y_A to base g so as we know that DLP is a

computational hard problem, and hence our scheme is secure.
The identity of Signer is computed as

$$ID_B = g^s mod p \tag{4.2}$$

so if an attacker wants to know the sign parameter s, he/she should be computing a discrete logarithm of ID_B base g so it is also a computational hard problem, so we can say that our scheme is secure.

4.1.2 Diffie-Hellman Problem

The diffie-hellman problem is a given prime p as a generator a given prime p and generator $g \epsilon Z_p^*$ and given that the element $g^m mod p$ and $g^n mod p$ it is hard to find $g^{mn} mod p$.The CDLP is treated as a hard computation problem reducible to DLP in a polynomial time. In our Algorithm, we have to used $g^{-\alpha} mod p$ and $g^{-\beta} mod p$, but the attacker cannot be able to calculated $g^{-\alpha * \beta} mod p$, so we can also assume here that based on CDHP, our scheme is secure.

4.1.3 Correctness

The blind signature s for a message M is indeed a valid signature. This can be checked with the help of ID_B.
Proof: The correctness of blind signature is given as below:
$(\mu^{t_1} Y_B^{t_2} g^{-\alpha} \mu g^{(-s\beta)}) = (g^l)^{(X_B (l)^{-1})} (g^{X_B})^{(s(X_B)^{-1})} (g^{-\alpha})(g^l)(g)^{(-s(\beta))}$
$g^{X_B} g^s g^{-\alpha} g^l g^{-(s\beta)}$
$Y_B g^s g^{-\alpha} g^{(\dot{s}+\dot{t}s)} g^{-(s\beta)}$
$Y_B g^{(s-\alpha)} g^{(\dot{s})+s(\dot{t}+\beta)} g^{-(s\beta)}$
$Y_B g^s g^{-\alpha} g^{\dot{s}+s\dot{t}+s\beta-s\beta}$
$Y_B g^s g^{-\alpha} g^{(\dot{s}+s\dot{t})}$
$Y_B g^{(s-\alpha+\dot{s}+s\dot{t})}$
$Y_B g^{(\dot{s}-\alpha)+s(1+\dot{t})}$
$Y_B g^{\ddot{s}+s(1+\dot{t})}$
$Y_B g^{\ddot{s}} ID_B^{(1+\dot{t})}$

Theorem 1: *It is impossible to create a valid signature.*

Proof: For creating a valid signature s attacker should know X_B,S_s both that imply attacker have control on both the parties that is likely to be impossible because in our scheme, both trusted party and signer are distinguishable even if both are not separate than also an attacker cannot create a valid signature so it is completely impossible to create it. Even trusted party also cannot forge s because he does not have any idea about X_B.

Theorem 2: *To determine the signer from two given signature is completely impossible.*

Proof: Suppose we have two messages M and N respectively signed by a signer. The proposed signature schemes are depended on DLP where we have

$$M, s_1, \lfloor M, \mu^{t_1} Y_B^{t_2} g^{-\alpha} \mu t_3^{\beta} \rfloor \tag{4.3}$$

$$N, s_2, \lfloor N, \mu^{t_1} Y_B^{t_2} g^{-\alpha} \mu t_3^{\beta} \rfloor \tag{4.4}$$

The above equations surely follow unlinkability as two signatures are hash or message digests along with a secret parameter of signer side as well as the user side so only the signature can be an analysis with the digest attacker or adversary cannot link the parameter, on the other hand, user side parameter α, β have random value so adversary cannot reveal anything about a signer.

Theorem 3:*No one can link the signature message pair even signer also cannot.*

Proof: The property of unlinkability also known as untraceable that emphasis on the tracability or linkability of the message-signature pair after publishing it. Untraceability is an important property of the blind signature scheme.

Supposed signer keeps the message signature pair

$$(\ddot{s}, \dot{t}, ID_B)$$

at the second glance it would be something like

$$(\ddot{s_1}, \dot{t_1}, ID_B)$$

. In our scheme as we used hash message along with some random parameter α, β so it is totally impractical to get the value of arbitrary parameter and after apply

the correct hash function. So for a malicious signer it is definitely impossible.

Theorem 4: *Trusted party as well as a signer both required equal authentication in our proposed work.*

Proof: As our design the identity of signer computed from the trusted party's public key Y_A thus trusted party will not deny his agreement. On the other situation signer identity involved in blinding. Therefore, the signer can be identified from his identity(IB_B), so after that signer did not deny his agreement also so we can say that trusted party as well as a signer both required authentication.

Theorem 5: *Our scheme satisfied the blindness property.*

Proof: We have to use the message blindness along with some signer's sent parameter that is t_1, t_2, t_3.After attached that parameter user also generated random parameter α, β and put it with an input message which should pass through the hash function all this combination is present by this equation

$$\dot{t} = H(m, \mu^{t_1} Y_B^{t_2} g^{-\alpha} \mu t_3^{\beta}) mod p \tag{4.5}$$

The hash function we are using in our scheme is SHA-2, which is the most secure message digest so if a malicious signer cannot reveal anything about a true message that's why we can say that our scheme satisfied blindness property as well.

Theorem 6: *Our scheme is verifiable.*

Proof: Our scheme can be verified by anyone after publishing the message signature pair $(\ddot{s}, \dot{t}, ID_B)$. it can be verified by that equation:

$$\dot{t'} = H(m, Y_B ID_B^{(1+\dot{t})} g^{\ddot{s}}) mod p \tag{4.6}$$

after calculating the value of $\dot{t'}$ it can be publicly checked if $(\dot{t'} = \dot{t})$. it is true than a pair is original otherwise rejected. So based on this our scheme is verifiable.

Theorem 7: *Our scheme shows resistance against side channel attack.*

Proof: First of all, we have to look what side channel includes, this attack consists of side channel information that is neither based the original message nor the digest, only some side information like time analysis of computing a phase or equation.Simple power variation or differential power variation will help out for

this attack [51].

Timing attack: Suppose we have runs a modular function in non fixed time total blind signature time must be correlated with the time

$$s = S_s + X_B modp \tag{4.7}$$

but further we know in our scheme S_s computed as

$$S_s = (k + rX_A) modp \tag{4.8}$$

where $r = g^k$ and they are generated by trusted party due to participation of the two-party parameters the modular computation completely synchronize to each other. The most significant bit of s are basically depended on $S_s \rightarrow X_B \rightarrow X_A$. So for knowing the first most bits you should know the trusted party as well as a signer but in our scheme, they both are transparent to each other. Suppose any condition the adversary has luck to get to identify both he/she must know every set of most bits that will be a computation hard problem. So we can say that our scheme has a good enough resistance against the time attack.

Theorem 8: *Our scheme has satisfied chosen Chiper text attack.*

Proof: Choosen chiper text attack model for which cryptanalysis the adversary gather information in a small part or at least a single part by choosing a chipertext and its secret under an unknown key [6, 9, 18].

Supposed the adversary wants to put a choosen chiper text attack so that he has to collect for parameter (c_1, c_2, c_3, c_4) and compute this equation

$$(c_1, c_2, c_3, c_4) = H(m, \mu^{t_1} Y_B^{t_2} g^{-\alpha} \mu t_3^{\beta}) modp \tag{4.9}$$

with

$$\mu = g^l modp \tag{4.10}$$

and

$$Y_B = g^{X_B} modp \tag{4.11}$$

in unblinding he used

$$v = atom(c_1^{X_B}.c_2^l) \tag{4.12}$$

if $c_4 = v$ then output should be $m = atom(c_1.c_3)$ else output rejects. Since we have to be used here cascading of four parameters the task to get a chipper text to another significant message unachievable at all because of computational hardness of DLP. If an adversary wants to choose random values for c_2, c_3, c_4 is also impossible to get it in infinite time for a computing manner. On the other scenario, message contains three parameter μ, t_1, t_2 that are further being complex because they are not directly calculated so it also meaning less the problem for an adversary to how would adjust nonlinear data. How will get a relevant relation.So it is completely secure against chosen chipper text attack.

4.2 Performance Analysis of Proposed Scheme

The complexity of all signature schemes generally emphasis on four operations namely inverse, multiplication, exponential operation and hash function. As we our well knowledge there is no other ID based blind signature scheme based on the discrete logarithm problem. So our scheme is novel that is why we have not compared to any other scheme.

In our analysis, we ignored the time to performing modular addition, and subtraction.

We have to used the following notation for analysis performance of our proposed scheme.

T_H is the computation time required for performing hash function.

T_I is the computation time required for inverse operation.

T_M is the computation time required for multiplication operation.

T_E is the computation time required for Exponential operation.

Table 4.1: Analysis of computational complexity

Blinding	Signature Generation	Signature Verification	Total
$4T_E + 4T_M + T_H$	$4T_E + 2T_I + 2T_M$	$2T_E + 2T_M$	$10T_E + 8T_M + 2T_I + T_H$

4.3 Chapter Summary

Our proposed scheme has to be analyzed with respect to many requirements, which have included correctness,unforgeability,untraceability,blindness,and distinguish of signer and trusted party and verifiability.

Our scheme has been passed all the test cases efficiently with respect to all security aspects. We have done performance analysis in second part of this chapter as our scheme is novel, so we need not compared it to with other schemes. Our proposed scheme has been implemented with java under some assumption described in next chapter.

Chapter 5

Implementation and result

5.1 Implementation

The implementation of our proposed scheme is done using java platform, and we have not been using any key storing concept in our algorithm so no need to use any database. We have done implementation using Itellij IDEA 13.1 as integrated development environment. In implementation of our scheme, we have to used java big integer value where security package and crypto packages for generating random number and secret key parameter for trusted party and signer, the hash function algorithm is used for blinding the message along with some random parameter by the user entity in blinding phase.

We have to generate prime number using the util package of java. Here we have used three party's namely trusted party, user and signer and the key parameter size is tested with 64 bits, 256 bits and 1024 bits. The message sizes are 5 KB and 8 KB. We have done the blinding of the message with the help of Hash function, SHA-2 is used in our implementation.
The standard hardware configuration(minimum) that should be supported is given as below:

1. Hard disk should be 150GB.

2. RAM should be 2GB.

3. OS can be users choose; we have to a used window platform system.

The implementation consists of following steps in the proposed scheme:

1. Setup

2. Extract

3. Blinding

4. Signature

5. Unblinding

6. Verification

The values for setup phases are given is bellow:

Generator g = 17406820753240209518581198012352343653860449079456135097849583104059995348845582314785159740894095072530779709491575949236830057425243876103708447346718014887611810308304375498519098347260155049469132948808339549231385000036164648264460849230407872187

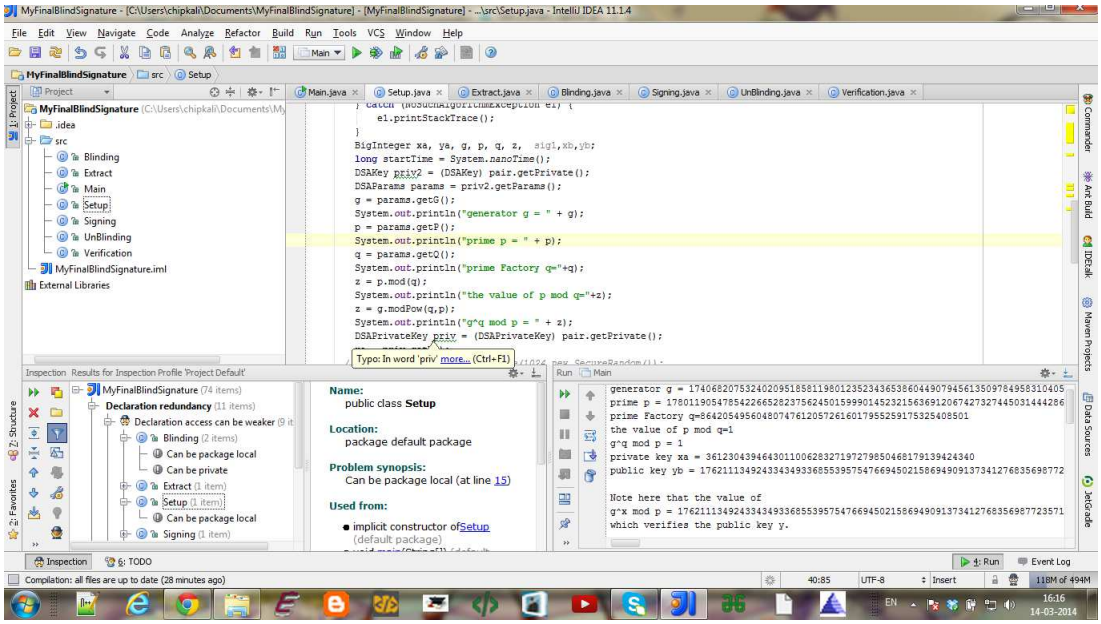

Figure 5.1: View of Setup Phase

189599990564960977693680177492737089620066891879567442107 30

Prime number p is p = 178011905478542266528237562450159990145232156369120674273274450314442 8

737020770612695252123463079567156784778466449970650770920727857050009668388144034129 74

522117181850604723115003930107995935806739534871706631980226201971496652413506094591 3707

594956514672855690606794135837542707371727429551343320695239

Prime Factor is q=864205495604807476120572616017955259175325408501

Check, whether the value of p and q is correct or not using the value of p mod q=1

Check, whether p, q, and g is a correct g^q mod p = 1

private key X_a = 409659790927730574991357522829154700552286323107

public key Y_A = 149339494482171125868162547464060894147958989777491727451347428826004656604 9512060723499650939378793788889656334006075993144393620157294899617278951039599476499 8900968359443324086905016929186040497936739970

079386961799304946474163166424054625060638410474375241425979420102682520169587149286 40752205929000837

Check, whether the value of X_A,Y_A is valid or not

g^{X_A} mod p = 149339494482171125868162547464060894147958989777491727451347428826004656604 0951206072349965093937879378888965633400607599314439362015729489961727895103959947649 9890968359443324086905016929186040497936739970079386961799304946474163166424054625060 63841047437524142597942010268252016958714928640752205929000837

Which verifies the public key Y_a.

K=387050839090005494030880584562763419807706397966

r=110626208380034464918750593221646602545954562578197307012077134891963907920060058955226995811348529659690806250620677107780259042421869557195260869449407290730607767954608676000514995483323523145068733487694159156721217083649103040823550015688105032133147726096570396644785014304774933103946058290950087862213

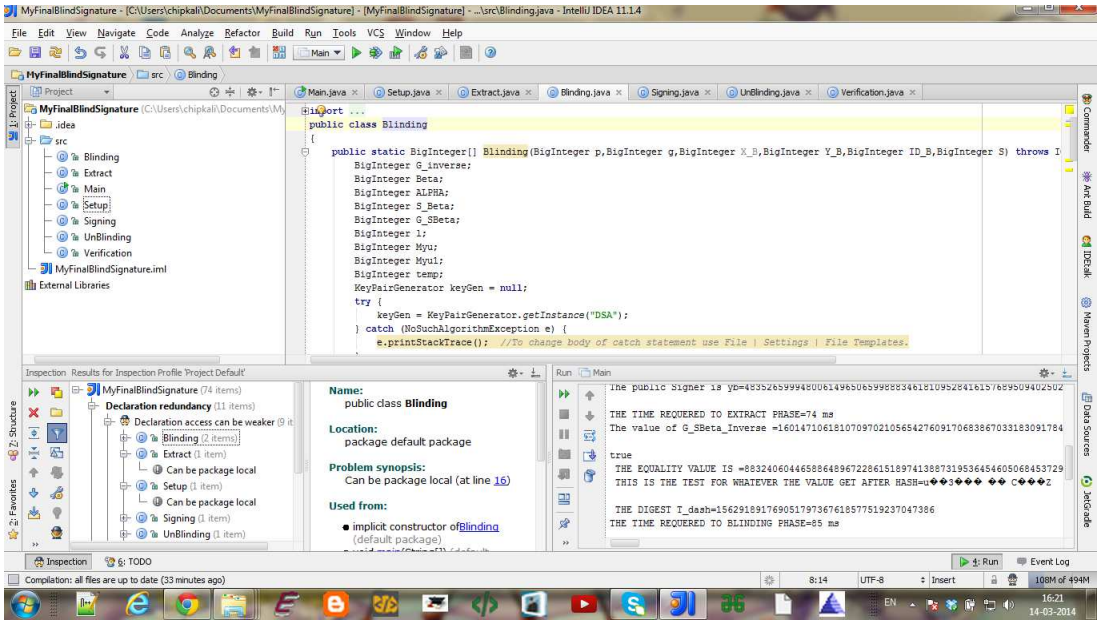

Figure 5.2: The view of Blinding

The value which we have given to hash at the time of message

blinding=97060361247266803493940727834290633792099744612313546640567620800068632513872659148788652396859769848514863966389370784916115883178214474879583282855901831466432414310925670589288842164979255085268207248090142574051988551943414769911775290025579944820837534890610603810596794378185975469399230918656210699894

The value what we get after hashing means it is nothing but the digest message.

HASH=31457285560270319608916306873335356137 0

The Digest $T^{'}$=31457285560270319608916306873335356137 0

This is the test for whatever the value get after hash=31457285560270319608916306873335356137 0

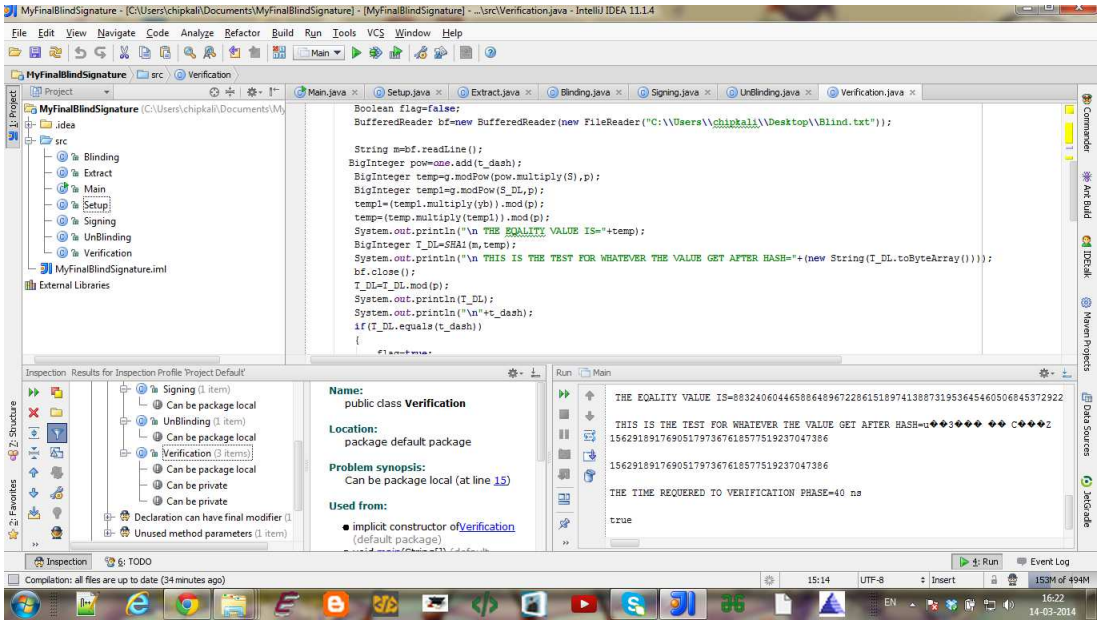

Figure 5.3: The view of Verification

Values in Verification Phase

$T^{'} = 3145728556027031960891630687333535613 70$

$T^{''} = 3145728556027031960891630687333535613 70$

5.2 Results

Analysis of Execution Time

The proposed scheme is implemented with processor intel(R)core(TM)i3 along with 3 GB RAM in using java as a programming language. We have calculated the time of each phase based using "System Time." Time". All phases have been implemented using fair system time on the same hardware on the same environment.

Table 5.1: Analysis of Execution time(msec)

Blinding	Signing	Verification	Keysize(Bytes)
1.7502 ms	0.005 ms	0.061 ms	8
20 ms	0.0099 ms	0.145 ms	10

Table 5.2: Analysis of Size of Signature in Bytes

Size of Message(Bytes)	Size of Signature(Bytes)
5000	8

5.3 Chapter Summary

All the Results and Implementation have been revealed in above section we got our algorithm is correct mathematically as well as programmatic way.The results can vary with other hardware and software environment.

Chapter 6

Conclusions and Future Work

We proposed an identity-based blind signature scheme that is having all security features with low computational overhead as well as feasible.We proved that our scheme has satisfied all the security goals of IDBS system like Unforgeability,Untraceability,Unlinkablity,Correctness,Verifiable and Blindness.As our best knowledge our we have given the first concept of this two notation together. In future our scheme can be used to get a fair system policy in e-commerce.With the help of our scheme a more secure E-cashing, E-voting, E-business can be build up in a great way.The given may be used for perfect crime avoidance also. All the faults of todays existing IDBS system has solved by our scheme.

Bibliography

[1] Shamir, Adi.Identity-based cryptosystems and signature schemes, Advances in cryptology, 47- 53, 1985.

[2] Huang, Zhenjie and Chen, Kefei and Wang, Yumin. Efficient identity-based signatures and blind signatures, Cryptology and Network Security, 120-133, 2005.

[3] Victor R. L. Shen, Yu Fang Chung, Tsar Shying Chen. A blind signature based on discrete logarithm problem, ICIC International, 5403-5416, September 2011.

[4] Li, Rupeng and Yu, Jia and Li, Guowen and Li, Daxing.A New Identity-Based Blind Signature Scheme with Batch Verifications, Multimedia and Ubiquitous Engineering, 2007. MUE'07. International Conference on, 1051- 1056, 2007.

[5] Sun, Hua. New Certificateless Blind Ring Signature Scheme, TELKOMNIKA Indonesian Journal of Electrical Engineering, 778 783, 2014.

[6] Boneh, Dan and Lynn, Ben and Shacham, Hovav. Short signatures from the Weil pairing, Advances in Cryptology ASIACRYPT 2001, 514-532, 2001.

[7] Jingfeng Su,Juxia Liu. A Identity Based Proxy Blind Signature Scheme Based on DLP, Internet Technology and Applications, 2010 International Conference on, 1-4, September 2010.

[8] F. Li, M. Zhang, and T. Takagi. Identity-based partially blind signature in the standard model for electronic cash Mathematical and Computer Modelling,2012.

[9] C.-I. Fan. Ownership-attached unblinding of blind signatures for untraceable electronic cash, Information Sciences, 176(3):263 -284, 2006.

[10] X. Yang and Z. Yu. An efficient proxy blind signature scheme based on dlp In Embedded Software and Systems, 2008. ICESS08. Pages 163-166. IEEE, 2008.

[11] D. He, J. Chen, and R. Zhang. An efficient identity-based blind signature scheme without bilinear pairings, Computers Electrical Engineering 37(4):444-450, 2011.

[12] J. L. Camenisch, J. M. Piveteau and M. A. Stadler. Blind signatures based on the discrete logarithm problem, Lecture Notes in Computer Science, pp.428-432, 1995.

[13] G. B. Agnew, R. C. Mullin and S. A. Van- stone Improved digital signature scheme based on discrete exponentiation, Electronics Letters, vol.26, 1024-1025, 1990.

[14] E. Mohammed, A. E. Emarah, Kh. ElShennawy.A Novel Blind Signature Using El- gamal, IEEE Arab Academy for Science and Technology, pages 189196. Air Defense Research Center, 2000

[15] X.Yang and Z.Yu.An efficient proxy blind sig- nature scheme based on DLP, ICESS 2008, pages 163-167, 2008.

[16] Z. W. Tan, Z. J. Liu, C. M. Tang. A proxy blind signature scheme based on DLP Journal of Software, 1931-1935, September 2003.

[17] Chen, Min Qin and Wen, Qiao Yan and Jin, Zheng Ping and Zhang, Hua. Secure and Efficient Certificateless Signature and Blind Sig- nature Scheme from Pairings, Applied Mechanics and Materials, 1262-1265, 2014.

[18] C. Rackoff and D. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attacks. In Advances in Cryptology-Crypto'91, LNCS 576, pp. 433-444. Springer-Verlag, 1991.

[19] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. SIAM J. Computing, 30(2):391-437, 2000.

[20] Xiaoming Hu,Shangteng Huang.Analysis of ID-based restrictive partially blind signatures and applications,The Journal of Systems and Software 81 (2008) 19511954.

[21] Chen, X.F., Zhang, F.G., Liu, S.L., 2007. ID-based restrictive partially blind signatures and applications. The Journal of Systems and Software 80 (2), 164171.

[22] Chaum, D., 1982. Blind signatures for untraceable payments. Advances in Cryptology Crypto82. Springer-Verlag, pp. 199203.

[23] S.M. Chow, C.K. Hui, S.M. Yiu and K.P. Chow, Two improved partyially blind signature schemes from bilinear pairings, ACISP 2005, LNCS 3574, Springer, pp. 316-328.

[24] Xiaofeng Chen , Fangguo Zhang and Shengli Liu. ID-based Restrictive Partyially Blind Signatures. Cryptology ePrint Archive, Report 2005/319.

[25] Li Hui-na,Ping Yuan, A simple one-time limited authorization mechanism based on ECDSA,ICACT'10,Pages 1580-1582.

[26] Wang Shaobin,Zhu Xian,Optimistic Fair-exchange Protocols Based on DSA Signatures,IEEE Computer Society(2004)Pages 498-501.

[27] MingHsin Chang,MingTe Chen,Design of Proxy Signature in ECDSA,ISDA '08,Pages 17-22

[28] Huang Tao, Zhang Le,Li Zhongjun,An Improved Scheme for E-signature Techniques Based on Digital Encryption and Information Hiding,ISIP '08,Pages 593-597.

[29] X. ming and S.Huang,Secure IDBS Scheme in the Standard Model,JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 26, 215-230 (2010).

[30] W.DIFFIE AND M.E.HELLMAN,New directions in cryptography,IEEE Trans.Inform. Theory,IT-22,6(1976) pp. 644-654.

[31] S.G.and J.K.,Almost all primes can be quickly certified,Proc.18th Annual ACM Symposium on the Theory of Computing, Berkeley,CA,1986.

[32] M. Agrawal, N. Kayal and N. Saxena,Primes is in P,Annals of Mathematics, 2002,Pages 781-793.

[33] A. ROYand S. KARFORMA,A survey on digital signatures and its applications,J. of Comp. and I.T. Vol. 3(1and2), 45-69 (2012).

[34] L.rivest,Adi shamir,M.adleman,Cryptographic communications system and method,Sep 20, 1983.

[35] A. Noore,A Secure Conditional Access System using DSE,Pages 7803-7721 2003 IEEE.

[36] M.khalil,M.Nazrin,Implementation of SHA-2 hash function for a DS SoC in FPGA,IEEE 2008.

[37] I.Te chen,Design of Proxy Signature in ECDSA,ISDA '08, Volume 03 Pages 17-22.

[38] Y. Qin,C.li and Y.china,A fast ECC DS based on DSP,Page(s):V7-83 - V7-86,IEEE 2009.

[39] Yu.Mu,W.Susilo,J,Zhou,Preserving transparency and accountability in optimistic fair exchange of DS,IEEE 6-2011.

[40] H. Y. Chien, J. K. Jan and Y. M. Tseng, RSA-based partially blind signature with low computation, IEEE, pp.385-389, 2001.

[41] C. C. Lee, An untraceable blind signature scheme, IEICE pp.1902-1906, 2003.

[42] L. Harn, Group-oriented threshold DS scheme and DMS, IEEE, vol.141, no.5, pp.307-313, 1994.

[43] L. J. Wang, J. J. R. Chen, Novel DSMS, ICIC, pp.1251-1256, 2010.

[44] K.A.ajmath,T.gowri,An IDBS Scheme from Bilinear Pairings,IJCSS volume(4),2003.

[45] D. Boneh and M. Franklin, IDE from the Weil pairing, in Proceedings of Crypto, LNCS 2139, 2001, pp. 213-229.

[46] F. Zhang, K. Kim, IDBS and ring signature from pairings,LNCS 2501,Springer Verlag, 2002, pp.533-547.

[47] F. Zhang, K. Kim, Efficient IDBS and PS from bilinear pairings, ACISP2003 , Springer-Verlag, 2003, pp.312-3323.

[48] L. Zhang,X. Tian,Novel Identity-based BS for Electronic Voting System,2010 Second International Workshop on Education Technology and Computer Science .

[49] Ni.Zhang,Jian Ping,ID-based Proxy blind signature scheme with unlinkability,DOI:10.1109/ICEICE.2011.

[50] S. Prabhadevi, A. M. Natarajan,Utilization of IDB Proxy BS Based on ECDLP in Secure Vehicular Communications IJEIT,, November 2013.

[51] Y. Zhou, D. Feng,Side-Channel Attacks, The NNSF of P.R. China,2010.

Dissemination of Work

Communicated

Journals

1. **Lokendra Rewapati**, and Sujata Mohanty. *Identity Based Blind Signature using Discrete Logrithm Problem*, Preprint submitted to International Journal of Electronics and Communications, Elsevier publication